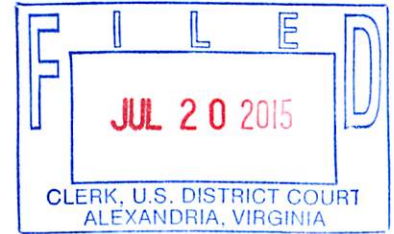


UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, *et al.*,

Plaintiffs,

v.

JOHN DOES 1-8,

Defendants.

Case No. 1:14-cv-00811 (LO/IDD)

**REPORT AND RECOMMENDATION**

This matter is before the Court on Microsoft Corporation (“Microsoft”) and FS-ISAC, Inc.’s (collectively, “Plaintiffs”) Motion for Default Judgment and Permanent Injunction against John Does 1-8 (“Defendants” or “Doe Defendants”), pursuant to Rule 55(b) of the Federal Rules of Civil Procedure. (Dkt. No. 52.) After the Defendants, or a licensed attorney for the same, failed to appear at the hearing on March 13, 2015, the undersigned Magistrate Judge took this matter under advisement to issue this Report and Recommendation. Upon consideration of the Complaint, Plaintiffs’ Motion for Default Judgment and supporting documentation thereto, and relevant portions of the underlying record, the undersigned Magistrate Judge makes the following findings and recommends that Plaintiffs’ Motion be GRANTED.

**I. INTRODUCTION**

On June 27, 2014, Plaintiffs Microsoft and FS-ISAC, Inc. (“FS-ISAC”) brought this action, alleging Defendants control a malicious computer botnet, known as the Shylock botnet, which has infected a large network of internet users’ computers. (Dkt. No. 1.) Plaintiffs contend that Defendants have used various means to lure victims to access malicious botnet code, which is secretly installed onto their computers. Defendants are then able to relay instructions to the

infected computers to conduct unauthorized activities, including stealing personal and online banking information. (Br. Supp. Default. J. at 2.) Plaintiffs claims are based on violations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030; Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2701; Lanham Act, 15 U.S.C. §§ 1114, 1125(a), (c); and, common law trespass to chattels, unjust enrichment, and conversion.<sup>1</sup> (Dkt. No. 1.) Plaintiffs now move for the entry of default judgment and a permanent injunction prohibiting Defendants from operating the Shylock botnet, and transferring ownership of the malicious botnet domains to Microsoft. (Br. Supp. Default. J. at 2.)

#### **A. Jurisdiction and Venue**

This Court has subject matter jurisdiction over this action, pursuant to 28 U.S.C. § 1331, because this suit arises under federal statutes: the CFAA, 18 U.S.C. § 1030; ECPA, 18 U.S.C. § 2701, and the Lanham Act, 15 U.S.C. §§ 1114, 1125. (Compl. ¶ 17.) This Court may also properly exercise supplemental jurisdiction over Plaintiffs’ remaining common law claims, pursuant to 28 U.S.C. § 1367. (*Id.*)

This Court may exercise personal jurisdiction over the Defendants, pursuant to Virginia Code § 8.01-328.1(A)(1). Plaintiffs assert that Defendants have availed themselves of the privilege of conducting business in the Commonwealth of Virginia by engaging in the alleged harmful acts through computers, internet websites, and instrumentalities located in Virginia. (Compl. ¶¶ 18-19.) Plaintiffs also assert that Defendants have affirmatively directed malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia. (*Id.*) Furthermore, certain Shylock botnet domains maintained by Defendants are

---

<sup>1</sup> Plaintiffs have not pursued their Sixth Claim for Relief, under the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C § 1962(c), in their Motion for Default Judgment.

registered through VeriSign and the Public Interest Registry, which are located in the Eastern District of Virginia. (Compl. ¶ 20.)

Venue is also proper in this Court, pursuant to 28 U.S.C. § 1391(b), because a substantial part of the events or omissions giving rise to Plaintiffs' claims, as well as a substantial part of the property that is the subject of Plaintiffs' claims, are situated in this district. (Compl. ¶¶ 18, 21.) Additionally, a domain name is deemed to have its situs in the judicial district in which the domain name registry that registered or assigned the domain name is located. As previously stated, VeriSign and Public Interest Registry are located in this judicial district. (Compl. ¶ 20.) Therefore, this Court may properly exercise jurisdiction over the Defendants.

#### **B. Service of Process**

On June 27, 2014, the District Judge found good cause to enter an *Ex Parte* Temporary Restraining Order ("TRO") disabling the command and control infrastructure Defendants have used to operate the Shylock botnet. (Dkt. No. 16.) Plaintiffs were ordered to serve the Defendants with copies of the TRO, the Complaint, and notice of a subsequent preliminary injunction hearing

by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon [D]efendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

(*Id.* at 14.) On July 8 and 14, 2014, Plaintiffs served the pleadings and papers in this action, in English and Russian languages, to all e-mail addresses known to be associated with the Shylock

botnet. (Dkt. No. 48-1 ¶ 7; Br. Supp. Default J. at 5.) Although the majority of these e-mail addresses were determined to be fake or had been closed, some were operational and successfully received the service e-mails. (*Id.*) On July 8, 2014, Plaintiffs also provided notice and service of the Complaint, Summons, and related documents, through a publicly available website: <http://botnetlegalnotice.com/shylock/>. (Dkt. No. 48-1 ¶ 8.) This website has remained online and accessible since July 8, 2014. (*Id.*)

On July 15, 2014, the Court found good cause to enter a preliminary injunction against the Defendants, and reiterated the directive to serve the Defendants with the pleadings and orders in this action by the means outlined above. (Dkt. No. 33 at 13.) On January 8, 2015, Plaintiffs re-served the Defendants at the functioning e-mail addresses identified during Plaintiffs' July 14, 2014 service attempt, as well as at fifteen additional e-mail addresses obtained through investigation of the Doe Defendants' identities. (*Id.* at ¶¶ 9-11.) Plaintiffs allege that these new e-mail addresses were used by Defendants to register Shylock botnet domains and IP addresses, and are the only available point of contact with Defendants. (Br. Supp. Default J. at 5-6.) Plaintiff confirmed through an e-mail tracking service that at least six of the service e-mails were delivered, opened, and read. (Dkt. No. 48-1 ¶ 12.)

Plaintiffs further assert that they have exhausted their ability to determine the Doe Defendants' true identities. (Br. Supp. Default J. at 5.) Plaintiffs' investigation yielded several names, addresses, e-mail addresses, and credit card account numbers associated with the Shylock botnet; however, these were later revealed to be fake or stolen. (Br. Supp. Default J. at 4.) Further investigation also led Plaintiffs to six individuals who they believed might have been associated with the Shylock infrastructure. (Dkt. No. 48-1 ¶ 5; Br. Supp. Default J. at 4-5.) These individuals reside in Saudi Arabia, Indonesia, Vietnam, Russia, and Canada. (Dkt. No. 48-1 at 2;

Br. Supp. Default J. at 5.) The individuals in Vietnam and Canada participated in telephone interviews with Plaintiffs, but neither was found to control the Shylock botnet infrastructure. (Dkt. No. 48-1 ¶ 5.) Moreover, these individuals did not have more specific information about the Doe Defendants' identities or contact information (*Id.*) The remaining individuals are beyond this Court's subpoena power, as Indonesia and Saudi Arabia are not signatories to the Hague Service Convention, and the Russian Federation no longer complies with formal requests for judicial assistance from the United States. (*Id.* at ¶¶ 5-6.)

Accordingly, the undersigned finds that Plaintiffs have complied with this Court's instructions regarding effectuating service upon the Defendants. Furthermore, the interruption of the Shylock botnet's infrastructure since the entry of this Court's TRO and preliminary injunction is reasonably calculated to notify Defendants of this action and, at a minimum, provide a basis for investigation if no notice had been received by other means. Thus, for the reasons stated above, the undersigned finds that service of process has been satisfied in this action.

### **C. Grounds for Entry of Default**

Plaintiffs filed the Complaint on June 27, 2014. (Dkt. No. 1.) The same day, Plaintiffs moved for, and the Court granted, an *Ex Parte* TRO. (Dkt. Nos. 5, 16.) The TRO was amended and executed on July 8, 2014, when Plaintiffs provided additional domain names and IP addresses associated with the Shylock botnet. (Dkt. Nos. 30, 32.) On July 15, 2014, the Court entered a preliminary injunction allowing Plaintiffs to disable the Shylock botnet's command and control infrastructure for the duration of this litigation, including by ordering that the domains registered by the Defendants resolve to Microsoft servers; transferring non-registered domains to the Plaintiffs; and, ordering U.S. internet service providers to block traffic to IP addresses and

domains associated with the Shylock botnet. (Br. Supp. Default J. at 6; Dkt. No. 33.) On July 23, 2014, the undersigned granted Plaintiffs' Motion for authorization to conduct discovery necessary to identify and serve the Doe Defendants.

Defendants have failed to appear, answer, or file any responsive pleading in this matter. On January 22, 2015, following the conclusion of Plaintiffs' discovery, Plaintiffs filed a Request for Entry of Default with the Clerk of the Court. (Dkt. No. 48.) On February 3, 2015 the District Judge instructed Plaintiffs to obtain a default from the Clerk and file an appropriate motion for default judgment. (Dkt. No. 49.) The Clerk entered default against Defendants on February 4, 2015. (Dkt. No. 50.) On February 19, 2015, Plaintiffs filed a Motion for Default Judgment and Permanent Injunction. (Dkt. No. 52.) When Defendants again failed to appear at the hearing on the Motion on March 13, 2015, the undersigned Magistrate Judge took the Motion under advisement to issue this Report and Recommendation.

## **II. FINDINGS OF FACT**

Upon a full review of the pleadings, the undersigned Magistrate Judge finds that Plaintiffs have established the following facts.

Microsoft is a Washington corporation with its principal place of business in Redmond, Washington. (Compl. ¶ 2.) Microsoft is a provider of the widely-recognized Windows® operating system, Internet Explorer® web browser, and other software and services. (Compl. ¶ 22.) Microsoft has invested substantial resources in developing and marketing high-quality products and services, and has generated substantial goodwill with its customers as a result of its strong branding. (*Id.*) The corporation holds registered trademarks for its famous brands, including Microsoft®, Windows®, and Internet Explorer®, with registration numbers 2872708, 2463526, and 2277112 respectively from the U.S. Patent and Trademark Office. (Dkt. No. 1-3.)

FS-ISAC is a Delaware non-profit corporation with its principal place of business in Reston, Virginia. (Compl. ¶ 3.) FS-ISAC is a trade organization comprised of 4,400 commercial banks, credit unions, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. (Compl. ¶ 23.) FS-ISAC's member institutions have also established a strong brand and substantial goodwill with their customers. (*Id.*) FS-ISAC was established in response to a 1998 Presidential Decision Directive, as amended in 2003, to allow the private and public sectors to share information about, prepare for, and respond to physical and cybersecurity threats to critical U.S. infrastructure. (*Id.*) The organization works closely with various government agencies, such as the U.S. Department of the Treasury, Department of Homeland Security, the Central Intelligence Agency, and state and local governments. (*Id.*)

Plaintiffs allege that Defendants are individuals that operate and control the Shylock botnets—identified as the USA, HJ-UK-1, HJ-UK-2, HJ-UK-3, HJ-UK-4, Net1, Net2, and Net3 botnets—in furtherance of activities designed to harm Plaintiffs, Plaintiffs' customers, and the general public. (Compl. ¶¶ 4-11.) Despite extensive investigation, Plaintiffs have been unable to discover the Doe Defendants' true identities.

A "botnet" is a collection of individual computers infected with malicious software ("malware") that allows communication among the computers, as well as centralized or decentralized communication with other computers providing control instructions. (Compl. ¶ 24.) The individual computers in a botnet often belong to users who have unknowingly downloaded or have been infected by this malware; for example, when the user inadvertently clicks on a malicious website advertisement or e-mail attachment, or downloads malware. (*Id.*) Once the malware code is downloaded or executed on the user's computer, the computer

becomes part of the botnet and is capable of sending and receiving communications, code, and instructions to or from other botnet computers. (*Id.*) Some botnets are wholly within the control of the botnet creators, and are referred to as “command and control” computers. (Comp. ¶ 25.) Botnets have the ability to support a wide range of illegal conduct without the owner of the compromised computer’s knowledge or consent, such as carrying out the theft of credentials and other personal information; computer intrusions; anonymously sending unsolicited bulk e-mail; delivering malware to other computers; or, to “proxy” or relay internet communications in order to obscure or conceal the true source of communications originating from other computers. (Compl. ¶ 26.)

Plaintiffs allege that Defendants are engaged in such illicit activities through the use of the Shylock botnet. (Compl. ¶ 29.) Specifically, Shylock-infected computers are used to gain unauthorized access to credentials for online banking websites, as well as to attack and infect other computers on the internet. (Compl. ¶¶ 29, 47.) Plaintiffs contend that when a user of a Shylock-infected computer attempts to log onto a financial institution’s website, the Shylock botnet secretly hijacks the user’s web browser, captures the user’s online financial login credentials and other identifying information, and then relays this information back to Defendants. (Compl. ¶ 29.) Because of the surreptitious nature of the Shylock botnet, the user is unaware of Defendants’ control and surveillance of the computer, or the theft of the user’s identifying information, banking credentials, or money from the user’s accounts. (*Id.*)

The Shylock botnet has a two-tiered structure: the lowest “Infection Tier,” followed by the “Command and Control Tier.” (Br. Supp. Default J. at 3; Compl. ¶¶ 31-37.) The Infection Tier consists of user computers infected with Shylock malware that perform day-to-day illegal activities. (Br. Supp. Default J. at 3.) The Command and Control Tier, however, consists of



specialized computers Defendants use to communicate with computers in the Infection Tier once an internet connection is established. (*Id.*) The Command and Control Tier relies on IP addresses, internet domains, and domain name servers to continuously control the Shylock-infected computers. (*Id.*; Compl. ¶ 35.)

A Shylock attack begins when an infected user computer attempts to connect to a financial institution's website. (Comp. ¶ 39.) The Shylock botnet detects this activity, which can be usurped in several ways. Plaintiffs allege that Shylock may record the keystrokes used to login to the banking website, record the information displayed on the website, or take a screenshot or video of the user's browsing session or account pages. (*Id.*) This information is then uploaded to computers in the Command and Control Tier, and can be used to attempt to steal additional account information or conduct other illegal activities. (*Id.*) A more sophisticated "web-inject" attack can also be used to extract sensitive information. (Comp. ¶ 40.) This occurs when additional code is injected into a website browser, allowing Shylock to alter the appearance of the financial institutions' webpage as it is displayed in the user's browser. (*Id.*) For example, where an authentic login page might only ask for the user's login ID and password, Shylock can extend this login process to ask for a social security number, birth date, mother's maiden name or other answers to confidential security questions, which are then recorded and transmitted to the Defendants. (*Id.*)

Additionally, Shylock is capable of displaying an entirely fake webpage for the financial institution the computer user is attempting to access. (Compl. ¶ 41.) As a result, the user believes she has connected to a real website and provides sensitive credentials to the fraudulent page. (*Id.*) Meanwhile, Defendants are able to use this information to access the user's accounts on the real website. (*Id.*) In order to complete the theft, Defendants can alter the transactions performed on

the real website, for example by changing withdrawal amounts or altering information related to where the money will be sent. (*Id.*) Because the attack is designed to mimic the financial institutions' webpages, including the institutions' trademarks, computer users are unaware that these activities are occurring, even as the Shylock botnet allows Defendants to access or empty users' bank accounts. (Compl. ¶¶ 43, 46.)

Consequently, the Shylock botnet causes harm to Plaintiffs and their customers in several ways. The malware infects computers by making changes at the "deepest and most sensitive levels" of the computers' operating systems, including the Windows Registry. (Compl. ¶ 48.) This alters the normal and approved settings and functions of the user's operating system to forcibly draw the computer into the Shylock botnet. (*Id.*) The clandestine nature of the botnet's architecture also causes many customers to inadvertently associate the resulting, degraded performance of Microsoft products and software with the Microsoft® brand, because many customers are unaware that they have become the victim of Defendants' attacks. (Compl. ¶ 49.) FS-ISAC member institutions and their customers have also suffered financial losses as a result of Defendants' unlawful conduct. (Compl. ¶ 51.) Furthermore, Microsoft, FS-ISAC, and FS-ISAC's member institutions have devoted substantial resources to investigating and remediating the harm caused by the Shylock botnet, including identifying and cleaning customers' infected computers. (Compl. ¶¶ 50-51.)

Plaintiffs assert that the Court's TRO and preliminary injunction have been "extremely effective" in disrupting the Shylock botnet's command and control infrastructure. (Br. Supp. Default J. at 7.) Plaintiffs now move for default judgment and seek a permanent injunction prohibiting Defendants from sending malware code and content from specified internet domains in furtherance of the alleged fraudulent conduct. (Dkt. No. 56.)

### III. EVALUATION OF PLAINTIFFS' COMPLAINT

Rule 55 of the Federal Rules of Civil Procedure provides for the entry of default judgment when a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend. *See Music City Music v. Alfa Foods, Ltd.*, 616 F. Supp. 1001, 1002 (E.D. Va. 1985). Foremost, a court must be satisfied that the complaint states a legitimate cause of action. *See Anderson v. Found. for Advancement, Educ. & Emp't of Am. Indians*, 155 F.3d 500, 506 (4th Cir. 1998) (holding that the district court erred in granting default judgment to the plaintiff where the plaintiff failed to state a claim). A defendant in default concedes the factual allegations of the complaint. *See, e.g., Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001); *see also Partington v. Am. Int'l Specialty Lines Ins. Co.*, 443 F.3d 334, 341 (4th Cir. 2006) (noting default judgment has the effect of admitting factual allegations in the complaint). Default does not, however, constitute an admission of the adversary's conclusions of law, and is not to be "treated as an absolute confession by the defendant of his liability and of the plaintiff's right to recover." *Ryan*, 253 F.3d at 780 (quoting *Nishimatsu Constr. Co., Ltd. v. Houston Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975)). Instead, the court must "determine whether the well-pleaded allegations in [the plaintiff's] complaint support the relief sought in [the] action." *Id.* at 780.

Thus, in issuing this Report and Recommendation, the undersigned Magistrate Judge must evaluate Plaintiff's claims against the standards of Rule 12(b)(6) of the Federal Rules of Civil Procedure to ensure that the Complaint contains plausible claims upon which relief may be granted. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (explaining the analysis for examining a plaintiff's claims under a 12(b)(6) motion to dismiss). To meet this standard, a complaint must set forth sufficient factual matter, accepted as true, "to state a claim to relief that is plausible on

its face.” *Id.* (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In determining whether allegations are plausible, the reviewing court may draw on context, judicial experience, and common sense. *Francis v. Giacomelli*, 588 F.3d 186, 193 (4th Cir. 2009) (citing *Iqbal*, 556 U.S. at 679.)

#### **A. First Claim for Relief: Computer Fraud and Abuse Act Violations**

The CFAA provides that a party will be penalized who: intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer, 18 U.S.C. § 1030(a)(5)(A); or, intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss, 18 U.S.C. § 1030(a)(5)(C). A “protected computer” is a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications with the United States.” 18 U.S.C. § 1030(e)(2)(B).

The CFAA was designed to prohibit the type of unauthorized access and fraudulent conduct facilitated by malware and botnet activity. *See, e.g., Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 636 (E.D. Va. 2009) (allegation that defendant accessed user’s e-mail account with credentials that did not belong to him actionable under the CFAA); *Physicians Interactive v. Lathian Sys., Inc.*, No. 03-1193-A, 2003 WL 23018270, \*5-\*7 (E.D. Va. Dec. 5, 2003) (finding cause to grant temporary restraining order and preliminary injunction for violation of the CFAA, among other counts, where defendant allegedly hacked into plaintiff’s secure website and stole confidential information).

Here, Plaintiffs have pled sufficient facts demonstrating that its customers' computers are "protected computers" under the CFAA, and that Defendants knowingly and intentionally accessed these computers in order to transmit malicious botnet code. The Shylock botnet's infrastructure allows Defendants to take control of victim's computers without their knowledge, and to commandeer these machines to carry out Defendants' illicit activities. Plaintiffs allege that the computers owned by victims of Shylock attacks are situated in this judicial district. The unlawful activities include the extraction and theft of sensitive, personal information, as well as the theft of funds from user bank accounts. The intrusion on these computers also includes accessing Windows® operating systems and Internet Explorer® software, and is done without the consent or authorization of Plaintiffs or their customers. This causes damage to Plaintiffs' customers' computers. Plaintiffs further allege that their losses within a one-year period amount to at least \$5,000 each. (Compl. ¶ 69.) Therefore, the undersigned finds that Plaintiffs have pled facts properly establishing Defendants' violation of the CFAA.

#### **B. Second Claim for Relief: Electronic Communications Privacy Act Violations**

The ECPA prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." <sup>2</sup> 18 U.S.C. § 2701(a). Although the term "facility" is not defined in the statute, the ECPA incorporates the definitions set forth at 18 U.S.C. § 2510. 18 U.S.C. § 2711(1). Therefore, an "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510(15). The term "electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or

---

<sup>2</sup> Section 2701 *et seq.* of the ECPA is also known as the Stored Communications Act, 18 U.S.C. §§ 2701–2712.

electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17). Obtaining stored electronic information from a facility through which electronic communication services are provided through the use of botnets, malware, and other malicious electronic entry violates this Act. *See, e.g., Global Policy Partners*, 686 F. Supp. 2d at 635-37 (unauthorized access to e-mails actionable under the ECPA); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 317-18 (E.D. Va. 2009) (unauthorized access to password-protected computer database a basis for ECPA claims).

Plaintiffs have alleged sufficient facts substantiating their ECPA claim against Defendants. Microsoft’s servers, the Windows® operating system, and Internet Explorer® software are facilities through which electronic communication services are provided. Plaintiffs allege that the Shylock botnet is used to hijack victims’ internet browsers and lead unsuspecting users to access fraudulent webpages. Plaintiffs also contend that, at the Defendants’ direction, the Shylock botnet intercepts communications without authorization while they are in transit and in storage in order to steal from computer users’ bank accounts and FS-ISAC member institutions. (Compl. ¶¶ 73-75.) Moreover, Plaintiffs have demonstrated how the surreptitious nature of the Shylock botnet is damaging to the Plaintiffs’ brands and the customer goodwill engendered by their products and trademarks. Therefore, the undersigned finds that Plaintiffs have established their claim under the ECPA.

### **C. Third, Fourth, and Fifth Claims for Relief: Lanham Act Violations**

Plaintiffs contend that Defendants are liable for violations of certain provisions of the Lanham Act, specifically: trademark infringement, under 15 U.S.C. § 1114; false designation of origin, under 15 U.S.C. § 1125(a); and, trademark dilution by tarnishment, under 15 U.S.C. § 1125(c). (Compl. ¶¶ 78-95.)

The Lanham Act prohibits the use in commerce of “any reproduction, counterfeit, copy, or colorable imitation of a registered mark,” without the consent of the registrant, “in connection with the . . . distribution, or advertising of any goods or services on or in connection with such use is likely to cause confusion, or to cause mistake, or to deceive.” 15 U.S.C. § 1114(1)(a). A defendant may be held liable for trademark infringement under this provision for the unauthorized use of a registered trademark in connection with online activity or software and website code. *See, e.g., Otels, Inc. v. Altun*, No. 1:11-cv-604, 2012 WL 3522616, \*4-\*5 (E.D. Va. June 13, 2012), *report and recommendation adopted*, 2012 WL 3522611 (E.D. Va. Aug. 14, 2012) (unauthorized use of a registered trademark in defendant’s website domain name deemed likely to cause confusion among consumers in violation of 15 U.S.C. § 1114(1)); *Brookfield Commc’ns. v. W. Coast Entm’t Corp.*, 174 F.3d 1036, 1055, 1066-67 (9th Cir. 1999) (directing preliminary injunction to be entered where trademark infringement was found to encompass unauthorized use of a registered mark in defendant’s software and website code.)

Additionally, the Lanham Act prohibits the use in commerce of “any false designation of origin, false or misleading description of fact, or false or misleading representation of fact” which is likely to cause confusion, mistake, or deceive “as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.” 15 U.S.C. § 1125(a)(1).

Trademark dilution by tarnishment is defined in 15 U.S.C. § 1125(c)(2)(C) as “association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.” The Lanham Act further provides:

Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner’s mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution . . . by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

15 U.S.C. § 1125(c)(1).

Here, Plaintiffs have pled facts demonstrating that Defendants’ conduct has violated provisions of the Lanham Act. The Shylock botnet generates and uses unauthorized copies of Microsoft’s registered and famous trademarks, as well as the trademarks of the financial institutions represented by FS-ISAC. During a Shylock attack, these counterfeit marks deceive computer users into believing they are using legitimate versions of the Windows operating system and are accessing Plaintiffs’ bona fide websites. The Shylock botnet is also intentionally misleading and confusing regarding Plaintiffs’ affiliation with and approval of Defendants’ malicious activities. Plaintiffs have devoted significant resources to remedying the damage caused by the Shylock botnet, as customers who experience the negative effects of a Shylock attack may attribute poor performance by Microsoft software, or other forms of identity and financial theft perpetrated by Defendants, with the Plaintiffs’ products and brands. Accordingly, Plaintiffs have alleged sufficient facts establishing Defendants’ liability for the misuse of Plaintiffs’ trademarks, dilution of the famous marks, as well as conduct that amounts to false designation of the origin of Defendants’ unlawful activities.



#### **D. Seventh, Eighth, and Ninth Claims for Relief: Common Law Tort Violations**

Finally, Plaintiffs seek to hold Defendants' liable for common law trespass to chattels, conversion, and unjust enrichment. (Compl. ¶¶ 106-27.)

##### **1. Trespass to Chattels and Conversion**

"A trespass to chattels occurs when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "the chattel is impaired as to its condition, quality, or value." *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998) (citations omitted) (internal quotation marks omitted). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." *Simmons v. Miller*, 544 S.E.2d 666, 679 (Va. 2001). The intrusion into an individual's computer system through hacking, malware, and unwanted spam e-mail communications may form the basis for claims of trespass to chattels and conversion. *See, e.g., Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (senders of bulk, spam e-mail committed trespass to chattels when they "caused contact with [plaintiff's] computer network" without authorization, and such contact "injured [plaintiff's] business goodwill and diminished the value of its possessory interest in its computer network."); *Physicians Interactive*, No. 03-1193-A, 2003 WL 23018270, at \*9 (finding a likelihood that defendant's alleged computer hacking attacks to obtain proprietary information were "designed to intermeddle with personal property in the rightful possession of [p]laintiff.")

Here, Plaintiffs allege that Defendants have committed trespass to chattels and conversion by using the Shylock botnet specifically to gain unauthorized access to users' computers, FS-ISAC member institutions' computer networks, and Microsoft's proprietary

Windows® operating system and Internet Explorer® software. Once infected with the Shylock botnet, Defendants are able to exercise control over users' computers, and monitor users' activities without their consent. Shylock botnet code is also designed to interfere with the most sensitive levels of a computer's operating system, which causes the machine to malfunction and diminishes the value and quality of the property. These actions cause injury to Plaintiffs' and their customers not only in terms of degraded computer performance, but also due to the theft of money from FS-ISAC financial institutions and extraction of login credentials from unsuspecting victims of Shylock attacks. Therefore, the undersigned finds that Plaintiff has pled sufficient facts to impose liability on Defendants for trespass to chattels and conversion.

## **2. Unjust Enrichment**

Plaintiffs assert that Defendants have been unjustly enriched with profits stolen from victims of the Shylock botnet. (Compl. ¶¶ 114-20.) To establish a claim for unjust enrichment, a plaintiff must show: (1) plaintiff's conferring of a benefit on the defendant; (2) defendant's knowledge of the conferring of the benefit; and, (3) defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." *Nossen v. Hoy*, 750 F. Supp. 740, 744-45 (E.D. Va. 1990).

These factors are satisfied in this case. Defendants control the malicious Shylock botnet in order to collect personal information from Plaintiffs' customers without consent. Defendants are aware that they derive a benefit from their unauthorized and unlicensed use of Microsoft's software and Plaintiffs' customers' computers because Defendants initiated this unauthorized use. By clandestinely installing malware onto users' computers, Defendants are able to take control of web browsers and search engines to direct users to fake webpages mimicking Plaintiffs' bona fide products and services. Defendants profit from the access the Shylock botnet

provides to unwitting users' sensitive personal information, as well as funds held by FS-ISAC financial institutions. It would be inequitable for Defendants to retain the benefits of this unlawful scheme. Thus, the undersigned finds that the facts as alleged are sufficient to state a claim for unjust enrichment.

#### **IV. REQUESTED RELIEF**

Plaintiff requests that this Court grant default judgment against Defendants, and enter a permanent injunction pursuant to Fed. R. Civ. P. 65. For the foregoing reasons, the undersigned finds that Plaintiffs are entitled to this relief.

#### **V. RECOMMENDATION**

For the reasons set forth above, the undersigned Magistrate Judge recommends that the Plaintiffs' Motion for Default Judgment and Permanent Injunction be **GRANTED**. The undersigned further recommends that the terms of the preliminary injunction entered by this Court on July 15, 2014 be converted into a permanent injunction—as outlined in Plaintiffs' proposed order—thereby enjoining Defendants, their representatives and persons who are in active concert or participation with them, from engaging in any of the activity complained of in this action, or causing any of the injuries complained of in this action; or aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of in this action, or causing any of the injury complained of in this action. Defendants should forfeit ownership and control of the command and control domains identified in Appendix A to this Report and Recommendation for transfer to Plaintiff Microsoft's ownership.


#### **VI. NOTICE**

**By mailing copies of this Report and Recommendation, the parties are notified that objections to this Report and Recommendation, pursuant to 28 U.S.C. § 636 and Rule 72(b)**

of the Federal Rules of Civil Procedure, must be filed within fourteen (14) days of service on you of this Report and Recommendation. A failure to file timely objections to this Report and Recommendation waives appellate review of the substance of the Report and Recommendation and waives appellate review of a judgment based on this Report and Recommendation.

The Clerk is directed to send a copy of this Report and Recommendation to all counsel of record.

Furthermore, Plaintiffs are hereby **DIRECTED** to post a copy of this Report and Recommendation on <http://botnetlegalnotice.com/shylock/>, and to send a copy of this Report and Recommendation to Defendants by electronic means and/or personal delivery, as has been done in accordance with the Court's past instructions regarding service on Defendants. Plaintiffs shall then file a notice with the Court indicating the date and manner in which such service has been completed.

 /s/ \_\_\_\_\_  
Ivan D. Davis  
United States Magistrate Judge

July 20, 2015  
Alexandria, Virginia

**APPENDIX A**

**.BIZ DOMAINS**

**Registry**

NeuStar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States

NeuStar, Inc.  
Loudoun Tech Center  
46000 Center Oak Plaza  
Sterling Virginia 20166  
United States

**Hardcoded Domains**

fastrackcrowlingss.biz  
fieldsocrossing.biz  
midjunelists.biz  
rotatingads.biz

**Configuration File Domains**

express-shippingus.biz  
modern-shipping.biz  
skylineinc-inc.biz  
topchoiceshippinginc.biz

**Money Mule Domains**

artable.biz  
brandnewshippinginc.biz  
bstrategic.biz  
business-shipping.biz  
capital-business-systems.biz  
client-spec-usa.biz  
consolidated-holdingsuk.biz  
dft-shipment.biz  
enterprise-holdingsuk.biz  
express-shippingus.biz  
fastlaneshipping.biz

financeconsulting-inc.biz  
finmurano.biz  
firstchoice-inc.biz  
first-consultansinc.biz  
flyhigh-inc.biz  
globalconnect-inc.biz  
global-holdings.biz  
global-techsolution.biz  
globeshippinginc.biz  
groupholdings-ltd.biz  
highland-holdingsltd.biz  
inn-technology.biz  
internetresources-us.biz  
interprolimited.biz  
inttechus.biz  
it-business-inc.biz  
itglobalserv-ltd.biz  
it-solutions-inc.biz  
jtsolutionsinc.biz  
leveauxgroupinc.biz  
mancapconsulting-ltd.biz  
modern-shipping.biz  
newlinesolutionsinc.biz  
new-source-unlimited.biz

new-york-finance.biz  
novatex-finanze.biz  
outsource-consultingus.biz  
outsourcemarketing-us.biz  
parcelzoneinc.biz  
partner-fingroup-inc.biz  
postexpressinc.biz  
primary-internationalltd.biz  
rexship-llc.biz  
sa-consulting.biz  
shiplandllc.biz  
shippinglineinc.biz  
skylineinc-inc.biz  
stroutsourcing.biz  
topchoiceshippinginc.biz  
tradeglobe-ltd.biz  
usacapital-oneoutsourcing.biz  
usa-financial-trust.biz  
us-internationalgroup.biz  
usparcelservice.biz  
wirelessgenerationinc.biz  
zonecapitalinc.biz

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)**  
**1775 Wiehle Avenue**  
**Suite 200**  
**Reston Virginia 20190**  
**United States**

**Hardcoded Domains**

**expressshipping.org**  
**durationuninstaller.org**  
**sterchelloness.org**

**Configuration File Domains**

**ac-shippingllc.org**

**Money Mule Domains**

**ac-shippingllc.org**  
**artcolors-ltd.org**  
**art-for-anyone.org**  
**baltic-shippingexpress.org**  
**expressshipping.org**  
**fbf-services.org**  
**feature-solutionuk.org**  
**finance-counts-uk.org**  
**fintechin-program.org**  
**horwardexpress-shipping.org**

**interpride-ltd.org**  
**it-campaign.org**  
**king-inntech.org**  
**premier-group-ltd.org**  
**stock-holderz-uk.org**  
**transaction-innovations.org**  
**uk-accessgroup.org**  
**ukpower-ltd.org**  
**usparcelservice.org**

**.COM, .NET, .CC DOMAINS**

**Registry**

**Verisign Naming Services  
21345 Ridgetop Circle  
4th Floor  
Dulles, Virginia 20166  
United States**

**Verisign Global Registry Services  
12061 Bluemont Way  
Reston Virginia 20190  
United States**

**Hardcoded Domains**

abp.cc  
acow.cc  
ac-shippingllc.com  
adix.cc  
adra.cc  
afn.cc  
agra.cc  
ahthuvuz.cc  
aingo.cc  
ajo.cc  
akf.cc  
alphard-info.net  
ambi.cc  
amia.cc  
asale.cc  
avar.cc  
bgx.cc  
big-web-svcs.cc  
bo0keego.cc  
bogs.cc  
cene.cc  
ciz.cc  
ckr.cc  
coob.cc  
coti.cc  
cuapoemi.cc  
cutes.cc  
cvl.cc  
deit.cc  
deloxnerviox.net  
doks.cc  
drg.cc  
duti.cc  
dvo.cc  
dza.cc

edal.cc  
eewuiwiu.cc  
eilahcha.cc  
elg.cc  
enp.cc  
e-protection.cc  
erp-cloud.cc  
estat.cc  
eux.cc  
eym.cc  
fiq.cc  
fooyuo.cc  
gah.cc  
gdm.cc  
giuchito.cc  
gmz.cc  
goc.cc  
guodeira.cc  
gva.cc  
iestats.cc  
ihl.cc  
ioh.cc  
irm.cc  
isohotel.net  
jeo.cc  
jub.cc  
kico.cc  
kinz.cc  
kirr.cc  
kity.cc  
kls.cc  
kre.cc  
lej.cc  
liem.cc  
lji.cc  
mbn.cc

mch.cc  
mkn.cc  
mny.cc  
mwr.cc  
nafe.cc  
nbh.cc  
nel.cc  
nitecapvideo.net  
nmbc.cc  
ognelisblog.net  
omp.cc  
onei.cc  
online-upd.net  
oonucoog.cc  
oras.cc  
orx.cc  
paly.cc  
pare.cc  
perahzoo.cc  
pfh.cc  
pmr.cc  
puv.cc  
rgf.cc  
rgk.cc  
rhk.cc  
rwn.cc  
sags.cc  
smis.cc  
soks.cc  
solt.cc  
sorg.cc  
sted.cc  
tohk5ja.cc  
tram.cc  
uab.cc  
ubd.cc

uceebeel.cc  
 updbrowser.com  
 uvo.cc  
 vbp.cc  
 veeceefi.cc  
 visite-mexico.net  
 wahemah.cc  
 wownthing.cc  
 coob.cc  
 stik.cc  
 buna.cc

### **Configuration File Domains**

express-shippingus.net  
 flyhigh-inc.net  
 rexship-llc.net  
 skylineinc-inc.net  
 solutionshippinginc.com  
 topchoiceshippinginc.net  
 useushippinginc.com

### **Plug-in Domains**

agy.cc  
 envy-svcs.cc  
 fooyuo.cc  
 hoks.cc  
 ohyeaahh.cc  
 safety-for-all.cc

### **Money Mule Domains**

1st-consultansinc.net  
 ac-shippingllc.com  
 adestaventurez.com  
 advanced-techinc.cc  
 aiwae.cc  
 aiwae.com  
 aiwae.net  
 artable-ltd.com  
 artable-uk.net  
 artcolors-ltd.com  
 artcolors-ltd.net  
 art-yard-uk.com  
 avid-techresources.cc  
 avid-techresources.com  
 avid-techresources.net  
 baltic-shippingexpress.com  
 bestway-solutions.com  
 bestway-solutions.net  
 bidei.cc  
 brandnewshippinginc.net

businesschoicellc.net  
 business-shipping.net  
 capitalbusiness-systems.com  
 chahuz.com  
 client-specusa-inc.net  
 consolidated-holdingsuk.net  
 cyndirocks.com  
 dft-shipment.net  
 enterprise-holdingsuk.com  
 enterprise-holdingsuk.net  
 enterprisetechinc.com  
 enterprisetechinc.net  
 equitytech-partners.cc  
 equity-techpartners.com  
 equitytech-partners.net  
 eshipperus.com  
 express-shippingus.net  
 fastlaneshipping.net  
 fbf-services.net  
 finacial-futures.net  
 financeconsultinginc.net  
 financeheads.com  
 fincounts-ltd.com  
 finmarintltd.cc  
 finmarint-ltd.net  
 finmurano.com  
 finmurano.net  
 fintechin-program.com  
 fintech-inprogram.net  
 fin-trustinc.com  
 firstchoice-inc.net  
 first-consultansinc-usa.com  
 flyhigh-inc.net  
 global-techsolution.net  
 globalus-united.net  
 globeshippinginc.net  
 groupholdings-ltd.com  
 groupholdings-ltd.net  
 guojo.cc  
 highland-holdings-ltd.net  
 infotech-xpert.com  
 inn-technology.com  
 inn-technology.net  
 internetresources-us.com  
 interpride-ltd.com  
 interpride-ltd.net  
 interprofinance.com  
 inttechus.com  
 it-alliance-ltd.com  
 it-business-inc.net

it-genies.net  
 it-genies-limited.com  
 itglobalserv-ltd.com  
 itglobalserv-ltd.net  
 itg-solutions-ltd.com  
 itg-solutions-uk.net  
 it-investmentgrouppllc.com  
 it-made-easy-limited.com  
 it-made-easy-ltd.net  
 it-merge-ltd.com  
 itprofessionals-group.com  
 it-smart-uk.com  
 it-solutions-inc.net  
 jtsolutionsinc.net  
 king-innovative.com  
 king-innovative.net  
 labbarra-holdings.com  
 legalgeneralgroup-plc.com  
 leibi.cc  
 liverinvestments-ltd.com  
 liverinvestments-ltd.net  
 mabcomuk.com  
 mancapconsultingltd.com  
 mancapconsulting-ltd.com  
 meridian-international.net  
 meridianus-inc.com  
 modern-shipping.net  
 neopro-inc.com  
 neopro-inc.net  
 newlinesolutionsinc.net  
 new-source-unlimited.net  
 newyork-finance.net  
 novatex-finanze.com  
 novatex-finanze.net  
 nycfinanceinc.com  
 onlineshippinginc.net  
 originalconsultinginc.com  
 originalconsultinginc.net  
 outsource-consultingus.com  
 outsource-consultingus.net  
 outsource-marketing-us.com  
 outsourcemarketing-us.net  
 paradigmcore.net  
 parcelzoneinc.net  
 partner-financialgroup.com  
 personaltouch-us.com  
 personaltouch-us.net  
 postexpressinc.net  
 premier-group-ltd.com  
 primary-internationalltd.net



rexship-llc.net  
 rickolxpressshipping.com  
 sabi-consulting.com  
 sa-consulting.cc  
 shiplandllc.net  
 shippinglineinc.net  
 shippingxtrainc.com  
 shippingxtrainc.net  
 shoph.cc  
 sky-edgeitsolutions.cc  
 sky-edgeitsolutions.com  
 sky-edgeitsolutions.net  
 skylineinc-inc.net  
 solutionshippinginc.com  
 solutionshippinginc.net  
 stockholderzzz.com  
 stormiq.com  
 strategic-inc.net  
 stroutsourcing.com  
 stroutsourcing.net  
 systems-and-communications.com  
 systems-and-communications.net  
 technology-inc.net  
 topchoicesshippinginc.net  
 tradeglobe-ltd.com  
 tradeglobe-ltd.net  
 transaction-innovations.net  
 uk-accessgroup.com  
 uk-accessgroup.net  
 ukfeature-solutions.com  
 uk-financecounts.net  
 ukglobal-holdings.com  
 ukglobal-holdings.net  
 uk-infotech-xpert.net  
 uk-ns-free.cc  
 ukpower-ltd.com  
 uk-stock-holderz.net  
 united-technologiesusa.com  
 united-technologiesusa.net  
 usa-capital-one-outsourcing.com  
 usa-countrywide-financial.net  
 usa-financialtrust.net  
 usa-zonecapital.com  
 us-capital-business.net  
 useushippinginc.com  
 useushippinginc.net  
 us-internationalgroup.com

usstrategic-inc.com  
 vale-usshipping.com  
 wirelessgenerationinc.net  
 xohze.cc  
 xohze.com  
 zone-capital-usa.net

*Dedicated Name Server Domains*

abp.cc  
 adestaventurez.com  
 adix.cc  
 agra.cc  
 agy.cc  
 aiwae.cc  
 aiwae.com  
 aiwae.net  
 ajo.cc  
 akf.cc  
 alax.cc  
 alphard-info.net  
 ambi.cc  
 avar.cc  
 bara.cc  
 bestmanta.net  
 bidei.cc  
 bogs.cc  
 buna.cc  
 cas-gallery.net  
 ckr.cc  
 clickmonopoly.net  
 clickmonopoly.net  
 coob.cc  
 cs of .net  
 cude.cc  
 dc-storm.net  
 deloxnerviox.net  
 drg.cc  
 dvo.cc  
 dza.cc  
 edal.cc  
 elg.cc  
 eym.cc  
 fiq.cc  
 freg.cc  
 gah.cc  
 gdm.cc  
 goc.cc  
 hoks.cc  
 ihl.cc

isohotel.net  
 kico.cc  
 kls.cc  
 lanegovonline.net  
 lavo.cc  
 lej.cc  
 librarymdp.com  
 liem.cc  
 liveathcr.net  
 macdegredo.com  
 mahe.cc  
 mch.cc  
 merand.cc  
 micatoge.net  
 mikemanser.net  
 mkn.cc  
 mny.cc  
 mwr.cc  
 nafe.cc  
 nbh.cc  
 nintendowiionline.net  
 nitecapvideo.net  
 ognelisblog.net  
 omp.cc  
 onei.cc  
 oras.cc  
 orx.cc  
 paradigmcore.net  
 pare.cc  
 pikeautomation.net  
 prai.cc  
 puppy.cc  
 rgf.cc  
 rhk.cc  
 slac.cc  
 sted.cc  
 stik.cc  
 tram.cc  
 trendei.net  
 uab.cc  
 uvo.cc  
 veso.cc  
 visite-mexico.net  
 webercountyfairr.net  
 xidungee.cc  
 xohze.cc  
 xohze.com  
 zoneoffsilence.com  
 xidungee.cc

## **.SU DOMAINS**

### **Registry**

**Технический Центр Интернет**  
Ул. Зоологическая д.8  
123242, Москва  
Российская Федерация  
тел.: 737 92 95  
факс: 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

**Technical Center of Internet**  
Technical Center of Internet  
8, Zoologicheskaya str  
Moscow 123242  
Russian Federation  
Tel: +7 495 737 92 95  
Fax: +7 495 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

### **RIPN/РосНИИРОС**

Алексей Платонов  
Академика Курчатова пл., д. 1  
123182, Москва  
Российская Федерация  
тел.: 196 9614  
факс: 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

### **RIPN/Russian Institute for Development of Public Networks (ROSNIROS)**

Dr. Alexei Platonov  
1, Kurchatov Sq.  
Moscow 123182  
Russian Federation  
Tel: +7 499 196 9614, +7 499 196 7278  
Fax: +7 499 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

### **Hardcoded Domains**

aisuvied.su  
bern.su  
caf.su  
eca.su  
eprotect.su  
feat.su  
grs.su  
igate.su  
iprotect.su  
klr.su  
lbb.su  
sito.su  
tco.su  
vng.su  
wand.su

### **Plug-in Domains**

apb.su  
axr.su  
cif.su  
egu.su  
gaso.su

### **Money Mule Domains**

jan.su  
tech-support-llc.su

### **Dedicated Name Server Domains**

azr.su  
bcv.su  
cdn-store.su  
eimiecha.su

greencloud.su  
maw.su  
mue.su  
ohy.su  
rnz.su  
strong-service.su  
teighoos.su  
vun.su  
wbx.su  
wyp.su  
yiequeih.su  
yimgscores.su  
ahbee.su  
ajeic.su  
choop.su  
tagoo.su